Can Current Cyber Security Policies Meet NAS Security and Safety Needs?

Marie Stella, CISSP

mvstella_99@yahoo.com

202 685-3046

The views expressed in this presentation are those of the author and do not reflect the official policy or position of the National Defense University or the Federal Aviation Administration

Today’s Challenge

In a world of highly interconnected, complex systems, does the current Certification and Authorization Security model effective?

The Proposal

A major change in security policy is needed that is enterprise network-centric based and not machine based.

Brief History of Security

Pre 1998: Included in system engineering processes as redundancy, reliability, and availability – objective was integrity, authentication and confidentiality were not major issues for the NAS

Post 1998: Presidential Decision Directive (PDD) 63 mandated the critical infrastructures (included transportation) be protected as part of the economic viability of the country. Government systems must be protected by mandate, private systems by guidelines (temporarily),

Post September 11, 2001: Included homeland defense as an objective.

Security Legislative and Policy (L&P) History of the Post 9/11 Period

Public Law 107-347 (Title III, Federal Information Security Act of 2002 (FISMA)

Homeland Security Presidential Directive # 7, Critical Infrastructure Identification, Prioritization, and Protection

OMB Circular A-130 (Appendix III), Security of Federal Automated Information Resources

National Strategy for Securing Cyberspace 2003

Patriot Act 1 and 2

What Does L & P Say?

Government to continue securing systems they same way we did under PDD-63 – NIST/OMB guidance

Business will not be regulated – continue to follow best practices and support Information Sharing and Analysis (ISACs)

Added some solution based technologies such as biometrics for border patrol and the use of countermeasures on aircraft to prevent manpad attacks

US would consider pre-emptive cyber attacks as a defense mechanism

Overseeing the Government Process

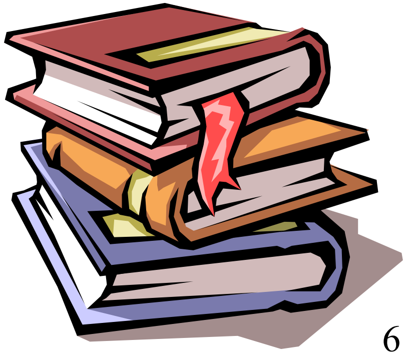
Government: National Institute of Standard (NIST)/National Security Agency – develops security processes for civilian systems, the Office of Management and Budget (OMB) ensures, through budget approval process, that processes are implemented.

Processes:

Certification and Accreditation of Federal Systems that include:

Risk Management Analysis

Funding (OMB's oversight)



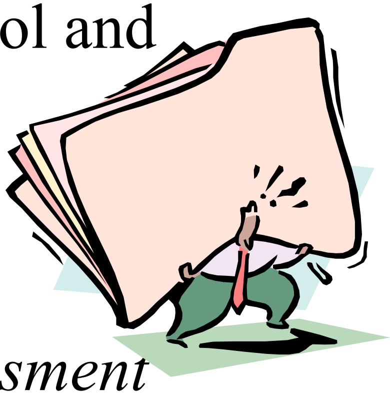
Tools to do the Job

SP 800-53-FIPS 200, Security Control Refinement

SP 800-18, Security Control Documentation

SP 800-60-FIPS199, Security Categorization

SP 800-37, System Authorization (C&A), control and monitoring



SP 800-53, Security Controls

SP 800-59, National Security

SP 800-53A, SP 800-37, Security Control Assessment

SP 800 –FIPS 200, Security Control Selections

(Tell you how to categorize, select, refine, document, implement, access, determine, authorize, monitor – document "vegematic")

Common Criteria

Testing and certifying systems in a certified testing lab against a pre-set list of security requirements being demonstrated in a specifically configured and set environment:

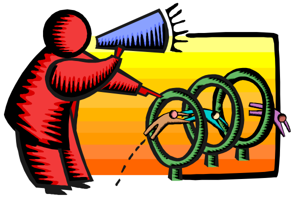
Check Point firewall – with back doors

Windows XP

Certification only applies to version tested, configuration tested and environment tested

L& P Government Impact

Cook Book process approach to Security



Very Expensive

Secures at the lowest level

Will get a program approved

L& P Business Impact

Heath Insurance Portability and Accountability Act (HIPPA) restrictions with accountability for privacy compromise

Rest of business – go forth and do good things!

Fraud and Espionage

Identity theft

Electric Grid Outages

Compromise and release of customer data

……

……

Are L&Ps Working?

NO!

WHY?

Lack of understanding of national IT security risk, asymmetric warfare,

No National Strategy and architecture for securing the critical infrastructure under cyber attack (and physical),

Policy, programs are becoming technology driven without understanding of implementation and political risks,

The IT State of the Union – legacy, COTS, range of trust, foreign developed software, no code insight, wireless, spectrum sale, focus on IP security,

No understanding of the threat models and agents and various range of attacks,

Poor economic and risk models for justifying security,

Minimal best practices underestimates costs and resources needed to secure infrastructure,

Lack of funding for research, education modernization, and quality of these activities,

Impact on ability to respond to attacks and future competitiveness of nation

What is the Fix?

National (International) AWARENESS – complexity and unpredictability of systems,

Develop a true national IT strategy – defense, homeland security, economic viability of the nation, and MANDATE it,

Funding and incentives for quality research in areas of complexity, emergent technologies, economic and risk modeling, fault tolerant systems, code Q&A,

Revision and Revival in technical education, especially in the area of engineering, to include network centric thinking,

Incentives for citizens and business (funding?) to keep IT market viable and secure systems globally, nationally and locally,

International agreements regarding security – early warnings, detection and isolation, forensics and accountability